No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

vs.

MICROSOFT CORPORATION,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF FORMER LAW ENFORCEMENT, NATIONAL SECURITY, AND INTELLIGENCE OFFICIALS AS *AMICI CURIAE* IN SUPPORT OF NEITHER PARTY

GUS P. COLDEBELLA
Counsel of Record
FISH & RICHARDSON P.C.
One Marina Park Drive
Boston, MA 02210
(617) 542-5070
coldebella@fr.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF THE ARGUMENT 3

ARGUMENT 4

I. The Unintended But Foreseeable Effects of Deciding Whether U.S. Warrants May Reach Data Stored Abroad 4

A. Conflicting Legal Obligations Will Lead to Less Efficient Law Enforcement and Intelligence Collection 4

1. Disclosure Obligations and Disclosure Prohibitions 4

2. Unilateral Disclosure Obligations Will Lead to Other Unilateral Disclosure Obligations 8

B. A Balkanized Internet 9

C. The Effect: Increased Political Repercussions and Reductions in Cooperation 14

II. This Case Is Not the Proper Vehicle for Fixing the Stored Communications Act 19

CONCLUSION 23

APPENDIX A: List of *Amici Curiae* 1a

TABLE OF AUTHORITIES

CASES **Page(s)**

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013) 21

Microsoft Corp. v. United States,
855 F.3d 53 (2d Cir. 2017) 20

STATUTES

Stored Communications Act,
18 U.S.C. §§ 2701-2712 ..... passim

Electronic Communications Privacy
Act, 18 U.S.C. §§ 2510 *et seq.* 7, 8, 21, 22

RULES

Sup. Ct. R. 37.3 2

Sup. Ct. R. 37.6 1

LEGISLATIVE MATERIALS

The Dynamic Gains from Free Digital Trade for the U.S. Economy: Hearing Before the Joint Econ. Committee,
115th Cong. (2017) 12

ECPA Modernization Act of 2017, S. 1657,
115th Cong. (1st Sess. 2017) 23

Email Privacy Act, H.R. 387,
115th Cong. (1st Sess. 2017) 22

Email Privacy Act, S. 1654,
115th Cong. (1st Sess. 2017) 22

Int'l Commc'ns Privacy Act, H.R. 3718,
115th Cong. (1st Sess. 2017) 22

Int'l Commc'ns Privacy Act, H.R. 5323,
114th Cong. (2d Sess. 2016) 22

Int'l Commc'ns Privacy Act, S. 1671,
115th Cong. (1st Sess. 2017) 22

Int'l Commc'ns Privacy Act, S. 2986,
114th Cong. (2d Sess. 2016) 22

Int'l Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcment: Hearing Before the H. Comm. on the Judiciary, 114th Cong. (2016).....5, 7, 14, 20

Int'l Data Flows: Promoting Digital Trade in the 21st Century: Hearing Before the Subcommittee on Courts, Intellectual Property, and the Internet, of the H. Comm. on the Judiciary, 114th Cong. (2015).....12

Letter from Peter J. Kadzik, Assistant Attorney General, U.S. Dep't of Justice, Office of Legislative Affairs, to The Hon. Joseph R. Biden, President of the U.S. Senate (July 15, 2016).....22

OTHER SOURCES

Alan Travis, *Drip Surveillance Law Faces Legal Challenge by MPs*, GUARDIAN, July 22, 2014 6

Alan Wehler, *Opinion: Microsoft Wins, Google Loses, and Confusion Reigns on Laws Surrounding Law Enforcement and Cloud Computing*, THE CHERTOFF GROUP, Feb. 7, 2017 20

Alan Wehler, *The Feds Need to Stop Using a 30-Year-Old Law to Access User Data Online*, THE HILL, Oct. 23, 2017 20

Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Info.*, NEWS, Sept. 28 2015.....11, 12

Anton Troianovski & Danny Yadron, *German Gov't Ends Verizon Contract*, WALL ST. J., June 26, 2014.....11

Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677 (2015).....10, 12

Claire C. Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014.....15

Data Localization Requirements Through the Backdoor? Germany's "Federal Cloud", and New Criteria for the Use of Cloud Services by the German Fed. Admin., NAT'L L. REV., Sept. 16, 2015 11

David Meyer, *Looks Like Data Will Keep Flowing From the EU to the U.S. After All*, FORTUNE, Feb. 2, 2016 18

Devlin Barrett & Danny Yadron, *Phone Protections Alarm Law Enforcement*, WALL ST. J., Sept. 22, 2014 15

European Commission, *Guide to EU-U.S. Privacy Shield*, 2016 17

Isabella Buono, *Mass Surveillance in the CJEU: Forging a European Consensus*, 76 CAMBRIDGE L.J. 250 (2017) 5, 6

Jabeen Bhatti, *In Wake of PRISM, German DPAs Threaten to Halt Data Transfer to Non-EU Countries*, BLOOMBERG BNA, July 29, 2013 17

Jennifer Daskal, *Issue Brief: Access to Data Across Borders: The Critical Role for Congress to Play Now*, AM. CONST. SOC'Y FOR L. & POL'Y, Oct. 2017 ..... 17, 20, 21

Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues* 8 NAT'L SEC. L. & POL'Y 473 (2016).....5, 9, 16

Johan Vandendriessche, *Case Translation: Belgium – Hof van Cassatie van België*, 13 DIG. EVID. ELEC. SIG. L. REV. 156 (2016) 8

John Leyden, *Russians Accuse FBI Agent of Hacking*, REGISTER, Aug. 16, 2002 18

Merkel and Hollande Mull Secure European Commc'n Web, DEUTSCHE WELLE, Feb. 16, 2014.....11

Michael Chertoff, *Cloud Computing Sets Stage for a Global Privacy Battle*, WASH. POST, Feb. 9, 2012 18

Michael Chertoff & Viet D. Dinh, *Michael Chertoff: Digital Security Requires a Legislative Overhaul*, TIME, Feb. 12, 2016.....17

Michael Chertoff, *Opinion: Data Localization is Misguided*, THE CHERTOFF GROUP, Mar. 29, 2017 10

Microsoft Announces Plans to Offer Cloud Services from German Datacenters, MICROSOFT NEWS CENTRE EUROPE, Nov. 11, 2015.....12

Nicholas Griffin, *Privacy v. Security*, 167 NEW L.J. 15, 16 (2017) 5

Nicole Perlroth & Scott Shane, *As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm*, N.Y. TIMES, Oct. 2, 2013 6

Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014) 7, 19, 20

Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) 20

Parmy Olson, *Encryption App Silent Circle Shuts Down E-mail Service 'To Prevent Spying'*, FORBES, Aug. 9, 2013 6

Paul Mozur et al., *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES, July 12, 2017 14

Paul Rosenzweig & David Inserra, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUNDATION, Apr. 1, 2014 15

Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Area of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017) 8, 16, 17, 21

Quantifying the Cost of Forced Localization, LEVIATHAN SEC. GRP., 2015 10

Remarks by APHSCT Lisa O. Monaco at the Int'l Conference on Cyber Security, July 26, 2016 14

Robert-Jan Bartunek, *Skype Loses Belgian Court Appeal After Fails to Comply with Call Data Order*, REUTERS, Nov. 15, 2017 8

Russia's New Personal Data Law Will Be Hard to Implement, Experts Say, MOSCOW TIMES, Sept. 1, 2015 13

Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, BLOOMBERG BNA, Aug. 10, 2015 13

Shaun Walker, *Russia Blocks Access to LinkedIn Over Foreign-Held Data*, GUARDIAN, Nov. 17, 2016 13

Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N.Y. TIMES, May 31, 2017 13

Sue-Lin Wong & Michael Martina, *China Adopts Cyber Security Law in Face of Overseas Opp'n*, REUTERS, Nov. 6, 2016 13

THE CHERTOFF GROUP, *Lawful Access to Data: A Critical Court Case in the United States and the Necessity of European Engagement*, Nov. 2017 8

Tom Bossert, Keynote Address at Center for Strategic and Int'l Studies Cyber Disrupt 2017 Summit: Next Steps for Cybersecurity After a Decade of Lessons Learned (Mar. 15, 2017) 10, 14

Tom Fox-Brewster, *WhatsApp Adds End-to-End Encryption Using TextSecure*, GUARDIAN, Nov. 19, 2014 15

Tom Risen, *Facebook Email Encryption Another Blow to Surveillance*, U.S. NEWS, June 2, 2015 15

INTEREST OF THE AMICI CURIAE[1]

Amici curiae are former national security, law enforcement, and intelligence community officials of the United States, the United Kingdom, and France, identified by name and former title in Appendix A.[2]

Amici have a continuing interest in combatting international crime and terrorism, protecting the privacy and civil liberties of their countries' citizens, and ensuring a U.S. legal framework that is clear for persons, companies, law enforcement entities, and our international partners.

---

[1] Letters consenting to the filing of this brief are on file with the Clerk. Pursuant to Supreme Court Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part, and no person, other than The Chertoff Group, led by *amici* former Secretary Chertoff and Chad Sweet, made any monetary contribution to the preparation or submission of this brief.

[2] The former affiliation of the *amici* with certain agencies is given here as biographical information. Their opinions have not been reviewed or endorsed by their respective former agencies, and the views expressed here are personal. Michael Chertoff, Chad Sweet, and Paul Rosenzweig, in their capacities at The Chertoff Group, advise technology clients including Microsoft who are affected by these issues, but these *amici* are submitting this brief on their own behalf. C. Stewart Verdery, Jr., in his capacity at Monument Policy Group, LLC, advises technology clients including Microsoft, but is submitting this brief on his own behalf. Peter Swire, as counsel to Alston & Bird LLP, has in the past provided legal advice to Microsoft, but is not representing Microsoft in the preparation or submission of this brief. Gus Coldebella is a Principal of Fish & Richardson P.C., which provides legal advice to Microsoft; however, Mr. Coldebella is not representing Microsoft in the preparation or submission of this brief.

Some *amici* have first-hand experience using the processes at issue here to seek user information from cloud service providers. Even so, *amici* are not asking the Court to rule one way or another. *Amici*'s brief is in support of neither party, and expresses no opinion on whether the Second Circuit correctly held that the warrant at issue calls for an impermissible extraterritorial application of the provisions of the Stored Communications Act ("SCA" or the "Act").[3] Instead, *amici* seek to assist the Court by identifying and explaining certain unintended but foreseeable consequences that are likely to flow from any decision in this case.

The Court has been asked to answer the question: do the SCA and existing law allow U.S. law enforcement to use a warrant to access user data stored on servers in a foreign country? But *amici* believe that the question that we, as a society, must answer is not whether current law allows it, but whether the law *should* allow U.S. law enforcement to use a warrant to access user data kept on servers in a foreign country—and, if so, how? Because courts necessarily adjudicate the rights of parties on a limited record, judicial resolution is not the optimal mode of answering this question. Legislative debate is. It is *amici*'s position that Congress, not the Court, is best suited to weigh the competing interests that this question presents—interests that include effective law enforce-

---

[3] In accordance with Supreme Court Rule 37.3, this brief is submitted within 7 days after the time allowed for filing the petitioner's brief because this *amicus curiae* brief is in support of neither party.

ment, national sovereignty, international comity, Internet openness and efficiency, commerce, and informational privacy.

Amici know that judicial consideration of the question presented is not designed to consider these multifarious interests, but a decision of this Court will have the same effect around the world as legislative action would: settling U.S. law on the subject and prompting action from both our international partners and our adversaries. This, we fear, will undermine—rather than enhance—the United States' and our allies' ability to enforce laws and maintain international cooperation.

SUMMARY OF THE ARGUMENT

At the same time the parties to this appeal are asking the Court to interpret the SCA, Congress is considering legislative amendments to the very provisions of the Act that gave rise to their dispute and this appeal. The SCA may or may not permit the United States to reach data stored outside of the United States via a warrant; *amici* take no position on this issue. But whatever the Court determines, it will have the effect of settling U.S. law on the extraterritorial reach of warrants seeking user data. We predict that such a ruling is likely to give rise to unintended consequences that will affect law enforcement and intelligence agencies, including the following:

- conflicting legal obligations across borders that compromise the effectiveness and efficiency of law enforcement and the international intelligence community;
- increasing balkanization of the Internet—a splintering of the World Wide Web via data localization, whether forced or voluntary—that

may curtail international law enforcement and inhibit intelligence cooperation; and

- an impetus for nations to move away from multilateral cooperation and toward a go-it-alone unilateralism, diminishing the cooperation of law enforcement and intelligence agencies around the world.

These risks are particularly worrisome given the critical role cooperation plays in tackling modern cross-border crime and cyberthreats—dangers that did not exist, or were not as virulent, decades ago.

Broad societal interests should be weighed to determine whether, and under what conditions, a domestic warrant may compel production of information from servers located on foreign soil. That balancing is a legislative, and not a judicial, function. As this Court has recognized, Congress is better suited than the Court to resolve questions that implicate America's relations with its fellow nations, and this is such a question.

ARGUMENT

I. The Unintended But Foreseeable Effects of Deciding Whether U.S. Warrants May Reach Data Stored Abroad

A. Conflicting Legal Obligations Will Lead to Less Efficient Law Enforcement and Intelligence Collection

1. Disclosure Obligations and Disclosure Prohibitions

A decision on the reach of a United States warrant to data stored abroad may exacerbate the risk that companies with an international presence are "forced

to choose between the laws of a nation that seeks production of data and the laws of another nation that prohibits such production."[4] Various disclosure obligations and prohibitions already simultaneously bind companies that hold customer data. Any increase in disclosure obligations by one country—such as allowing U.S. warrants to reach data stored on foreign soil—may be met by other countries with escalation of their own disclosure requirements.

It may also result in nations requiring countervailing disclosure *prohibitions*, to reaffirm their sovereignty over the perceived incursion.[5] This conflict between disclosure obligations and disclosure prohibitions is likely to put companies in a precarious position—as it already has when two legal regimes collide. For example, in 2014, the United Kingdom enacted the Data Retention and Investigatory Powers Act ("DRIPA").[6] DRIPA permitted the Home Secretary to require communication providers to retain unlimited metadata to enable the UK government's collection of data for certain "public policy purposes."[7] But in

---

[4] Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 NAT'L SEC. L. & POL'Y 473, 473 (2016).

[5] *Int'l Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 75-77 (2016) [hereinafter *Hearing*] (statement by Michael Chertoff, former Secretary of the U.S. Department of Homeland Security and Chairman of the Chertoff Group).

[6] Nicholas Griffin, *Privacy v. Security*, 167 NEW L.J. 15, 16 (2017).

[7] Isabella Buono, *Mass Surveillance in the CJEU: Forging a European Consensus*, 76 CAMBRIDGE L.J. 250, 250-53 (2017). In the United Kingdom, DRIPA was replaced by the Investigatory

2017, presumably in partial reaction to the leaks by Edward Snowden that resulted in international concern about U.S. intelligence collection, the EU Court of Justice held that such domestic legislation was *per se* incompatible with the privacy protections in the EU Charter of Fundamental Rights.[8]

This battle between norms is even more pitched when a company must comply with multiple and conflicting regimes, where complying with one set of laws leads to violating another. Before responding to lawful requests, companies are forced to seek the imprimatur of a court for fear of liability—leaving law enforcement and investigations in limbo until a decision issues and appeals are exhausted. And in the meantime, company employees are placed at risk of incarceration, or businesses choose to shutter altogether.[9] As the following examples demonstrate, ratcheting up

---

Powers Act ("IPA") in December 2016. The IPA replicated much of DRIPA. *Id.* *See also* Alan Travis, *Drip Surveillance Law Faces Legal Challenge by MPs*, GUARDIAN, July 22, 2014, *available at* https://www.theguardian.com/world/2014/jul/22/drip-surveillance-law-legal-challenge-civil-liberties-campaigners.

[8] Buono, *supra* note 7, at 250-53.

[9] Lavabit and Silent Circle are two examples of U.S. companies that chose to close their businesses in response to, or in anticipation of having to respond to, government requests for information under the current legal regime. *See* Nicole Perlroth & Scott Shane, *As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm*, N.Y. TIMES, Oct. 2, 2013, *available at* http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html; Parmy Olson, *Encryption App Silent Circle Shuts Down E-mail Service 'To Prevent Spying'*, FORBES, Aug. 9, 2013, *available at* https://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/#4b34419b6376.

these stakes only heightens the possibility of stalemate and further slows the flow and sharing of information; it does nothing to advance law enforcement and intelligence community objectives.

- In 2015, Brazilian authorities arrested a local Microsoft executive because the company refused to provide data to Brazilian law enforcement on the basis that it would violate U.S. law.[10] Brazilian authorities refused to seek this information through the Mutual Legal Assistance Treaty ("MLAT") process, despite Microsoft's position that disclosure of data stored in the U.S. would violate the Electronic Communications Privacy Act ("ECPA").[11]
- In 2007, Belgium criminally charged Yahoo! for failing to disclose records in connection with a probe into suspected criminal activity, even though Yahoo! argued that, as a U.S. provider, it was not subject to Belgian law but was bound to follow ECPA.[12] The Belgian Court of Cassation rejected Yahoo!'s position, holding that Yahoo! was obligated to cooperate with Belgium's law enforce-

---

[10] *See, e.g.*, *Hearing*, *supra* note 5, at 62 (statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp.) (testifying that Brazil has levied fines against Microsoft's local subsidiary and is pursuing criminal prosecution of a Microsoft executive in Brazil for Microsoft's compliance with U.S. law).

[11] *Id.*

[12] *See, e.g.*, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 408-09 (2014).

ment, though Yahoo! did not have an office in Belgium, and even if such cooperation—in Yahoo!'s view—violated the ECPA.[13]

- Just one month ago, Skype lost a Belgian court appeal for failing to comply with a request to share data from messages and calls. Skype maintained it could not provide such information because, among other reasons, the servers were based in Luxembourg, which could block such disclosure.[14]

2. *Unilateral Disclosure Obligations Will Lead to Other Unilateral Disclosure Obligations*

Settling the law on the reach of U.S. warrants may beget demands by foreign jurisdictions for data stored in the U.S. *Amici* are concerned about the rise of unilateralism, where countries opt to make their own decisions on how to handle foreign-stored data, as opposed to using existing, multijurisdictional means, such as the MLAT process.[15] As one scholar has observed:

---

[13] *See* Johan Vandendriessche, *Case Translation: Belgium – Hof van Cassatie van België*, 13 DIG. EVID. ELEC. SIG. L. REV. 156 (2016); *see also* THE CHERTOFF GROUP, *Lawful Access to Data: A Critical Court Case in the United States and the Necessity of European Engagement*, Nov. 2017, at 3.

[14] Robert-Jan Bartunek, *Skype Loses Belgian Court Appeal After Fails [sic] to Comply with Call Data Order*, REUTERS, Nov. 15, 2017, *available at* https://www.reuters.com/article/us-skype-belgium-court/skype-loses-belgian-court-appeal-after-fails-to-comply-with-call-data-order-idUSKBN1DF1MA.

[15] *See generally*, Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Area of Globalized Commc'ns: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017).

> The approach taken by the United States is likely to become a model for others, thus providing the United States a unique opportunity to set the standards—standards that ideally will protect privacy, security, and the growth of an open and global Internet. The alternative is a balkanized Internet and a race to the bottom, with every nation unilaterally seeking to access sought-after data, companies increasingly caught between conflicting laws, and privacy rights minimally protected, if at all.[16]

This trend may diminish cooperation and coordination among nations' law enforcement, and compound the dilemma of conflicting legal regimes.

B. A Balkanized Internet

To combat the unilateralism of other states, countries may implement compelled data localization—requiring data originating within a country to be stored within the nation's borders. As we have already seen, regulation in this area could require creation of local subsidiaries over which the host country can exercise jurisdiction to handle the data of that country's citizens. Even without data localization laws, technology companies may choose to house datacenters in foreign countries to avoid the conflict of laws issues described earlier.

Amicus and former Secretary of the U.S. Department of Homeland Security Michael Chertoff characterized data localization as "foreshadow[ing] the

---

[16] Daskal, *supra* note 4, at 474-75.

death knell of the global network as we know it."[17] Data localization erodes the open nature of the Internet by imposing costs and barriers for users to access and retrieve data. If widely implemented, data localization will diminish many network benefits—international commerce and trade, freedom of speech, instantaneous global communications, and political freedom—by reducing network access and making it more expensive to deliver services.[18]

Amici are concerned about these undesirable effects of data localization. Authoritarian governments use data localization to control and exercise power over their citizens by limiting the free exchange of information. Protectionist countries use data localization to exclude non-domestic companies from their economies, ostensibly to protect local industries, but to the detriment of other market participants and the purchasing power of their own citizens.[19]

---

[17] Michael Chertoff, *Opinion: Data Localization is Misguided*, THE CHERTOFF GROUP, Mar. 29, 2017, *available at* https://www.chertoffgroup.com/point-of-view/109-the-chertoff-group-point-of-view/651-opinion-data-localization-is-misguided.

[18] *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 679-82, 716-22 (2015) (describing how data localization "increas[es] costs and other burdens enormously for both providers and consumers and render[s] many of such global services impossible," while making foreign surveillance easier); *Quantifying the Cost of Forced Localization, Leviathan Sec. Grp.*, 2015 (discussing the cost of data localization, including decreased protection against national disasters).

[19] *See* Chander & Le, *supra* note 18, at 722-23, 735-36; *see generally* Tom Bossert, Keynote Address at Center for Strategic and Int'l Studies Cyber Disrupt 2017 Summit: Next Steps for Cybersecurity After a Decade of Lessons Learned (Mar. 15, 2017) ("I think those countries that are seeking data localization are misguided. . . . If it's a centralized function on behalf of the people

These effects are already occurring in countries that have adopted data localization measures. Germany has begun turning away from U.S. companies, such as Verizon, and toward state-owned entities, such as Deutsche Telekom, to route data through its domestic servers.[20] In February 2014, Chancellor Angela Merkel proposed building an internet infrastructure to keep data within Europe.[21] Germany subsequently announced plans to establish a German cloud infrastructure for the federal administration (the "Bundes-Cloud").[22] On the heels of these developments, companies such as Microsoft have chosen to

---

run by the government, you'll have tendencies surrounding data localization and the exclusion from our markets of other services and goods from other countries. Those are two things that are antithesis to our—to our fundamental U.S. values, if you will."); Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Info.*, NEWS, Sept. 28 2015, at 3-4, 7, *available at* https://www.albrightstonebridge.com/news/data-localization-challenge-global-commerce-and-free-flow-information (describing how data localization is not only costly, but will place companies and NGOs in a position that would either force them to abandon key markets or become complicit to the activities of authoritarian regimes).

[20] Anton Troianovski & Danny Yadron, *German Gov't Ends Verizon Contract*, WALL ST. J., June 26, 2014, *available at* https://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

[21] *Merkel and Hollande Mull Secure European Commc'n Web*, DEUTSCHE WELLE, Feb. 16, 2014, *available at* http://www.dw.de/merkeland-hollande-mull-secure-european-communication-web/a-17435895.

[22] See *Data Localization Requirements Through the Backdoor? Germany's "Federal Cloud", and New Criteria for the Use of Cloud Services by the German Fed. Admin.*, NAT'L L. REV., Sept.

locate datacenters for cloud services for Germany in Germany, presumably to avoid the fate of companies that store German citizens' information abroad.[23]

In France, the government has pushed for local datacenter infrastructure referred to as "le cloud souverain"—the sovereign cloud—to limit cloud services in France to French companies operating in France.[24] As part of this effort, France invested €150 million into two French companies—Numergy and Cloudwatt—to build a domestic French cloud infrastructure separate from those offered by other tech companies.[25]

Russia and China have gone even further. In September 2015, a Russian law took effect requiring "personal data operators" to restrict the collection, storage, and processing of any data about Russian users to databases located within Russia.[26] The Russian

---

16, 2015, *available at* https://www.natlawreview.com/article/data-localization-requirements-through-backdoor-germanys-federal-cloud-and-new.

[23] *Microsoft Announces Plans to Offer Cloud Services from German Datacenters*, MICROSOFT NEWS CENTRE EUROPE, Nov. 11, 2015, *available at* https://news.microsoft.com/europe/2015/11/11/45283/.

[24] *The Dynamic Gains from Free Digital Trade for the U.S. Economy: Hearing Before the Joint Econ. Committee*, 115th Cong. 41 (2017) (statement of Sean Heather, Vice President, Center for Global Regulatory Cooperation, U.S. Chamber of Commerce).

[25] *Int'l Data Flows: Promoting Digital Trade in the 21st Century: Hearing Before the Subcommittee on Courts, Intellectual Property, and the Internet, of the H. Comm. on the Judiciary*, 114th Cong. 34 (2015) (statement of Robert D. Atkinson, President, The Information Technology and Innovation Foundation).

[26] Albright Stonebridge Group, *supra* note 19, at 10-11; Chander & Le, *supra* note 18, at 701-02.

government announced that the law applies to all data operators that store personal data of Russian citizens, wherever located.[27] In November 2016, Russia blocked access to LinkedIn for supposed violations of the law.[28] Non-Russian companies still struggle to comply with the Russian law.[29]

China implemented a data localization law in June 2017, requiring operators of "critical information infrastructure" to store certain business data and personal information of Chinese citizens in China.[30] Following the trend of other companies moving user data to comply with China's data localization requirements, earlier this year Apple announced that

---

[27] Sergei Blagov, *Russia Clarifies Looming Data Localization Law*, BLOOMBERG BNA, Aug. 10, 2015, *available at* https://www.bna.com/russia-clarifies-looming-n17179934521/.

[28] Shaun Walker, *Russia Blocks Access to LinkedIn Over Foreign-Held Data*, GUARDIAN, Nov. 17, 2016, *available at* https://www.theguardian.com/world/2016/nov/17/russia-blocks-access-to-linkedin-over-foreign-held-data.

[29] *Russia's New Personal Data Law Will Be Hard to Implement, Experts Say*, MOSCOW TIMES, Sept. 1, 2015, *available at* https://themoscowtimes.com/news/russias-new-personal-data-law-will-be-hard-to-implement-experts-say 49268.

[30] Sue-Lin Wong & Michael Martina, *China Adopts Cyber Security Law in Face of Overseas Opp'n*, REUTERS, Nov. 6, 2016, *available at* https://www.reuters.com/article/us-china-parliament-cyber/china-adopts-cyber-security-law-in-face-of-overseas-opposition-idUSKBN132049; Sui-Lee Wee, *China's New Cybersecurity Law Leaves Foreign Firms Guessing*, N.Y. TIMES, May 31, 2017, *available at* https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html.

it would open a datacenter in China to comply with the law.[31]

C. The Effect: Increased Political Repercussions and Reductions in Cooperation

Information sharing—including cooperation across international boundaries and between the world's public and private sectors—is key to combatting present-day security issues, including the scourge of cyberattacks. As Michael Chertoff explained to Congress:

> Today, the Internet is a globe-spanning domain. More than three billion citizens and six billion devices are connected to the Internet. Its value proposition is that it is an open network of networks. As we work to preserve the openness of the Internet, we must do so through collaboration between the private sector, government, and the broader international community.[32]

---

[31] Paul Mozur et al., *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES, July 12, 2017, *available at* https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html.

[32] *Hearing*, *supra* note 5, at 76 (statement by Michael Chertoff, former Secretary of the U.S. Department of Homeland Security and Chairman of the Chertoff Group); *see also* Bossert, *supra* note 19 ("We need an effort that no longer looks at the bottom of the mountain but that rather looks in a higher topography order to get to the root cause of some of these botnet attacks. It's going to require the collaborative cooperation of companies—as you know, not only ISP providers. . . . Some are social media companies. Some are Internet search engines. But collectively, that information can be readily assessed, readily digested."); Remarks by APHSCT Lisa O. Monaco at the Int'l Conference on Cyber Security, July 26, 2016, *available at*

In the aftermath of the leaks perpetrated by Edward Snowden, companies have offered more robust encryption options to their customers.[33] Described by

---

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/remarks-aphsct-lisa-o-monaco-international-conference-cyber-security ("To put it bluntly, we are in the midst of a revolution of the cyber threat—one that is growing more persistent, more diverse, more frequent, and more dangerous every day. Unless we act together—government, industry, and citizens—we risk a world where malicious cyber activity could threaten our security and prosperity."); Paul Rosenzweig & David Inserra, *Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, HERITAGE FOUNDATION, Apr. 1, 2014, *available at* http://www.heritage.org/defense/report/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom ("By sharing information, different entities in the two sectors can be warned about likely attacks or specific problems in the software.").

[33] *See, e.g.*, Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J., Sept. 22, 2014, *available at* https://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341 (describing announcements by Apple and Google of new operating systems that would make it more difficult for law enforcement to retrieve data); Tom Risen, U.S. NEWS, *Facebook Email Encryption Another Blow to Surveillance*, June 2, 2015, *available at* https://www.usnews.com/news/articles/2015/06/02/facebook-email-encryption-another-blow-to-surveillance (reporting announcement by Facebook giving users more encryption options); Tom Fox-Brewster, *WhatsApp Adds End-to-End Encryption Using TextSecure*, GUARDIAN, Nov. 19, 2014, *available at* https://www.theguardian.com/technology/2014/nov/19/whatsapp-messaging-encryption-android-ios (reporting that WhatsApp messaging systems will now provide default end-to-end encryption); Claire C. Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014, *available at* https://www.nytimes.com/2014/03/22/busi-

the FBI as the "going dark" problem, this trend increases the importance to law enforcement of access to stored data, often located on servers in other countries.[34] As observed by at least one former member of President Obama's Review Group on Intelligence and Communications Technology, "the ability to track down perpetrators is high enough within the United States that it is only lucrative for spam rings to operate from overseas."[35] The cross-border nature of this and many other cybersecurity and cybercrime investigations further complicates the ability of law enforcement and intelligence community officials to efficiently acquire needed information.[36]

The consequence of this Court's decision will be a patchwork of competing laws, as detailed above, and acceleration toward data localization the world over. The U.S. settling this question will be particularly influential because it affects the global information network—a network that began in the U.S. and where U.S. companies have dominated since its inception.[37]

---

ness/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html ("Security analysts say tech companies have collectively spent millions and possibly billions of dollars adding state-of-the-art encryption features to consumer services, like Google search and Microsoft Outlook, and to the cables that link data centers at Google, Yahoo and other companies.").

[34] Swire & Hemmings, *supra* note 15, at 703, 707-08.

[35] *Id.* at 704.

[36] *Id.* at 703-04.

[37] Jennifer Daskal, *supra* note 4, at 474 ("While the problem of cross-border access to data is inherently international, the United States has an outsized role to play, given a combination of the U.S.-based provider dominance of the market, blocking provisions in U.S. law that prohibit the production of the content of electronic communications (such as emails) to foreign-based

At present, the United States receives more data requests from other countries than it makes itself.[38] International law enforcement and intelligence community cooperation is likely to diminish as other countries decide to take matters into their own hands through unilateral actions.[39]

Collateral commercial effects, such as challenges to the EU-U.S. Privacy Shield, are also near certain.[40] Because transfers of personal data are a necessary part of the global digital economy, the EU-U.S. Privacy Shield was created to permit such transfers contingent upon a company's agreement to abide by heightened data protection rules and safeguards.[41] A U.S. company's ability to comply, and to retain foreign

---

law enforcement, and the particular ways that companies are interpreting and applying their legal obligations.").

[38] Swire & Hemmings, *supra* note 15, at 700-01.

[39] Jennifer Daskal, *Issue Brief: Access to Data Across Borders: The Critical Role for Congress to Play Now*, AM. CONST. SOC'Y FOR L. & POL'Y, Oct. 2017, at 3, 6, 13, *available at* https://acslaw.org/sites/default/files/Access_to_Data_Across_Borders.pdf.

[40] The EU-U.S. Privacy Shield effectively replaced the more than 15-year-old U.S.-EU Safe Harbor Program, which allowed personal information of European citizens to be transferred to U.S. companies that self-certified compliance with EU data protection regulations. Michael Chertoff & Viet D. Dinh, *Michael Chertoff: Digital Security Requires a Legislative Overhaul*, TIME, Feb. 12, 2016, *available at* http://time.com/4218197/digital-security/; Jabeen Bhatti, *In Wake of PRISM, German DPAs Threaten to Halt Data Transfer to Non-EU Countries*, BLOOMBERG BNA, July 29, 2013, *available at* https://www.bna.com/wake-prism-german-n17179875502/.

[41] European Commission, *Guide to EU-U.S. Privacy Shield*, 2016, at 7, 10, *available at* http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf.

customers, may be jeopardized by the decision in this case. Related collateral effects on existing cooperative law enforcement arrangements, such as that between the United States and the European Union, may also come to pass.[42] At bottom, however, the most detrimental effect may be the attitudinal changes at the national leadership levels of law enforcement and intelligence teams, leading to decreased international cooperation in law enforcement and counterterrorism.[43] Such decreased cooperation may also come at the risk of increased foreign prosecution of members of the law enforcement and intelligence communities.[44]

---

[42] *See, e.g.*, David Meyer, *Looks Like Data Will Keep Flowing From the EU to the U.S. After All*, FORTUNE, Feb. 2, 2016, *available at* http://fortune.com/2016/02/02/looks-like-data-will-keep-flowing-from-the-eu-to-the-u-s-after-all/ (reporting that the EU-U.S. Privacy Shield was agreed to upon a U.S. promise that access to Europeans' data by the U.S. will be subject to "clear limitations").

[43] Michael Chertoff, *Cloud Computing Sets Stage for a Global Privacy Battle*, WASH. POST, Feb. 9, 2012, *available at* https://www.washingtonpost.com/opinions/cloud-computing-sets-stage-for-a-global-privacy-battle/2012/02/06/gIQAhV2V2Q_story.html?utm_term=.0352415d2cde.

[44] *See, e.g.*, John Leyden, *Russians Accuse FBI Agent of Hacking*, REGISTER, Aug. 16, 2002, *available at* https://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/ (reporting charges by Russia's Federal Security Service against an FBI agent for obtaining unauthorized access to computers in Russia as part of an FBI operation).

II. This Case Is Not the Proper Vehicle for Fixing the Stored Communications Act

This Court's declaration of what the Stored Communications Act means may lead to international changes, legal and practical, that overwhelm the policy considerations being considered by Congress. The debate over the ability of *one* law enforcement agency to obtain evidence in *one* case should not be the catalyst to a legal framework that may make it even more difficult for law enforcement and intelligence to do their jobs in cross-border investigations.

This is particularly true where the statute at issue is as distanced from modern reality as is the Stored Communications Act. When Congress drafted the SCA in 1986, its purpose was to protect the privacy rights of U.S. citizens when using remote communications and computing services in the United States.[45] The statute reflects the understanding and landscape of internet-based communications[46] at that time—a landscape that is vastly different today.[47] In 1986, the SCA was an achievement; more than thirty years later, its language and structure have been rendered obsolete by technological advances, including

---

[45] Kerr, *supra* note 12, at 404-10.

[46] The language of the Stored Communications Act describes these parties as "provider[s] of electronic communication service" and "remote computing service." 18 U.S.C. §§2701-2712. These designations, however, are difficult to map onto modern multifunctional network service providers, leading to confusion in the application of the Act. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213-15 (2004) (laying out the framework of the Stored Communications Act).

[47] *Id.* at 1214.

the advent of the World Wide Web, the development of a global Internet, the near-universal adoption of electronic mail and mobile phones, and the rise of cloud computing and data storage.[48] This case illustrates how the SCA's ill-fitting application to modern technology "has made it difficult for legislators to legislate in the field, reporters to report about it, and scholars to offer scholarly guidance."[49] Experts from technology, law enforcement, and the law generally agree that the SCA needs reform, and moreover that Congress is the appropriate body to do so.[50]

---

[48] Kerr, *supra* note 12, at 390-410 (laying out five different areas where the language of the statute is outdated because of changing technology, including the territoriality of the Act); *see also* Alan Wehler, *Opinion: Microsoft Wins, Google Loses, and Confusion Reigns on Laws Surrounding Law Enforcement and Cloud Computing*, THE CHERTOFF GROUP, FEB. 7, 2017, *available at* https://www.chertoffgroup.com/point-of-view/109-the-chertoff-group-point-of-view/636-opinion-microsoft-wins-google-loses-and-confusion-reigns-on-laws-surrounding-law-enforcement-and-cloud-computing.

[49] Kerr, *supra* note 46, at 1208.

[50] *Id.* at 1209; Kerr, *supra* note 12, at 416-18; Daskal, *supra* note 39; Alan Wehler, *The Feds Need to Stop Using a 30-Year-Old Law to Access User Data Online*, THE HILL, Oct. 23, 2017, *available at* http://thehill.com/opinion/technology/356668-the-feds-need-to-stop-using-a-30-year-old-law-to-spy-on-users-online; *Microsoft Corp. v. United States*, 855 F.3d 53, 55 (2d Cir. 2017) (Carney, J., concurring) ("We recognize . . . that in many ways the SCA has been left behind by technology. It is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose."); *Hearing*, *supra* note 5, at 72 (statement by Michael Chertoff, former Secretary of the U.S. Department of Homeland Security and Chairman of

One critical reason that Congress and not the Court should determine questions surrounding the reach of domestic warrants is that *any* result will have effects in the international sphere. This statute raises policy concerns that include the balancing of competing interests such as effective law enforcement (both domestic and foreign), national sovereignty, international comity, Internet openness and efficiency, commerce, and informational privacy.[51] The legislative process can take these factors into account and balance them, whereas this Court is restricted to the interpretation of a 31-year-old statute and the facts before it. For example, Congress could balance changes made to the SCA with those implemented in other areas, such as the Mutual Legal Assistance Treaties, by streamlining the MLAT process for cooperation between governments while, at the same time, adding privacy protections to the ECPA.[52]

This Court has repeatedly held that it is the role of Congress, and not the courts, to take the lead in international relations and weigh these competing interests. *See, e.g.*, *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664-69 (2013) ("The presumption against extraterritoriality guards against our courts triggering . . . serious foreign policy consequences,

---

the Chertoff Group) (testifying that these issues "are quite technical, and even having been a Federal judge, I have to say I am not sure the Federal courts in the first instance are the right place to resolve all of the competing issues in technical dimensions of these kinds of questions").

[51] Daskal, *supra* note 39.

[52] Swire & Hemmings, *supra* note 15, at 735 ("We also suggest that the concerns about lowering privacy protections as part of the streamlined MLA process might be accompanied by offsetting new privacy protections elsewhere in a reform of ECPA.").

and instead defers such decisions, quite appropriately, to the political branches.").

It is important to note that on this issue Congress has not stood idly by. Bipartisan legislation entitled the International Communications Privacy Act ("ICPA") was introduced to both houses of Congress in May 2016,[53] and proposed ICPA legislation has been reintroduced in both houses in the current Congress.[54] The United States Department of Justice has also presented to Congress draft legislation for addressing cross-border data requests.[55] These measures are under consideration by Congress, in addition to several other bills seeking to update the ECPA.[56]

---

[53] *See* Int'l Commc'ns Privacy Act, H.R. 5323, 114th Cong. (2d Sess. 2016) (sponsored by Rep. Marino [R-PA-10], and cosponsored by Rep. DelBene [D-WA-1]); Int'l Commc'ns Privacy Act, S. 2986, 114th Cong. (2d Sess. 2016) (sponsored by Sen. Hatch [R-UT], and cosponsored by Sen. Coons [D-DE] and Sen. Heller [R-NV]).

[54] *See* Int'l Commc'ns Privacy Act, H.R. 3718, 115th Cong. (1st Sess. 2017) (sponsored by Rep. Collins [R-GA-9] and cosponsored by Rep. Jeffries [D-NY-8], Rep. DelBene [D-WA-1], and Rep. Issa [R-Ca-49]); Int'l Commc'ns Privacy Act, S. 1671, 115th Cong. (1st Sess. 2017) (sponsored by Sen. Hatch [R-UT], and cosponsored by Sen. Coons [D-DE] and Sen. Heller [R-NV]).

[55] *See* Letter from Peter J. Kadzik, Assistant Attorney General, U.S. Dep't of Justice, Office of Legislative Affairs, to The Hon. Joseph R. Biden, President of the U.S. Senate (July 15, 2016), *available at* https://assets.documentcloud.org/documents/2994379/2016-7-15-US-UK-Biden-With-Enclosures.pdf.

[56] *See, e.g.*, Email Privacy Act, H.R. 387, 115th Cong. (1st Sess. 2017) (sponsored by Rep. Yoder [R-KS-3], and cosponsored by a bipartisan group of 138 additional representatives); Email Privacy Act, S. 1654, 115th Cong. (1st Sess. 2017) (sponsored by Sen

CONCLUSION

Amici believe that since the present case implicates only the facts and issues presented on appeal, it should not be used as a vehicle to address statutory defects requiring congressional attention. *Amici* thus request that the Court rule with these equities and interests in mind, and allow Congress to address the broader questions that are likely to have far-reaching international effects.

Lee [R-UT], and cosponsored by a bipartisan group of 7 additional senators); ECPA Modernization Act of 2017, S. 1657, 115th Cong. (1st Sess. 2017) (sponsored by Sen. Lee [R-UT], and cosponsored by Sen. Leahy [D-VT] and Sen. Daines [R-MT]).

Respectfully submitted,

GUS P. COLDEBELLA
Counsel of Record
CAROLINE K. SIMONS
CLAIRE COLLINS
FISH & RICHARDSON P.C.
One Marina Park Drive
Boston, MA 02210
(617) 542-5070
coldebella@fr.com

JACQUELINE TIO
FISH & RICHARDSON P.C.
1180 Peachtree St. NE,
21st Floor
Atlanta, GA 30309
(404) 892-5005

Counsel for Amici Curiae

APPENDIX

APPENDIX A: List of *Amici Curiae*

Joel F. Brenner, former Senior Counsel and Inspector General, National Security Agency; former National Counterintelligence Executive and Mission Manager for Counterintelligence

Judge Jean-Louis Bruguière, former Vice-President, Tribunal de Grande Instance (Investigating Magistrate and lead for the National Judicial Anti-Terrorist Division), France

Michael Chertoff, former Secretary, U.S. Department of Homeland Security

Gus P. Coldebella, former Acting General Counsel and Deputy General Counsel, U.S. Department of Homeland Security

Daniel Dell'Orto, former Principal Deputy General Counsel, U.S. Department of Defense

I. Lewis Libby, former Assistant to the Vice President for National Security Affairs; former Chief of Staff to the Vice President of the U.S.; former Assistant to the President

The Rt Hon. Lord Reid of Cardowan, former Vice-Chair of the All Party Parliamentary Group on Homeland Security; former Home Secretary; former Secretary of State for Defence, United Kingdom

Paul Rosenzweig, former Deputy Assistant Secretary of Policy, U.S. Department of Homeland Security

Chad Sweet, former Chief of Staff, U.S. Department of Homeland Security

Peter Swire, former Member, Director of National Intelligence Review Group on Intelligence and Communications Technologies; former Chief Counselor for Privacy, U.S. Office of Management and Budget

C. Stewart Verdery, Jr., former Assistant Secretary for Border and Transportation Security Policy and Planning, U.S. Department of Homeland Security